UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,377	12/12/2001	Ashley Anderson Brock	RSW920010214US1	2825

26502 7590 11/07/2005

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/015,377	BROCK ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 12/12/2001.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 15 and 16 appear to be directed to the data table, per se, which are non-functional descriptive material and not tangibly embodied.

Any other claims not addressed are rejected by virtue of their dependency

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 14 – 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Munson et al. (PN: 6681331).

As per claim 14, Munson teaches an intrusion detection system, comprising:

an event detector for detecting a system event (Munson: Column 4 Line 55 – 65);

a signature table comprising signatures (Munson: Column 4 Line 61 – 62: intrusion profile data is qualified as signatures); and

logic for searching the signature table responsive to detection of the system event by the event detector (Munson: Column 4 Line 60 – 65);

wherein the signature table includes at least one null signature and at least one signature that is not a null signature (Munson: Column 4 Line 30 – 33 and Column 4 Line 61 – 62: nominal execution profile is considered as a null signature).

As per claim 15, Munson teaches a signature table of an intrusion detection system, said signature table comprising a plurality of signatures, wherein at least one signature of the plurality of signatures includes occurrence data (Munson: Column 4 Line 30 – 65 and Column 5 Line 23 – 30: nominal execution profile is considered as a null signature).

As per claim 16 -- 18, the claim limitations are met as the same reasons as that set forth in rejecting claim 14 and 15.

4. Claims 1 – 11 and 19 – 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya (PN: 6279113).

As per claim 1, Vaidya teaches an intrusion detection method, comprising the steps of:

storing a plurality of signatures in a signature table of an intrusion detection system (Vaidya: Column 3 Line 40 – 45); and

ranking at least two signatures of the plurality of signatures by likelihood of occurrence (Vaidya: Column 11 Line 25 – 28, Column 11 Line 34 – 36 and Column 11 Line 48 – 51: the likelihood of occurrence is based on the timely sequence of events that may occur during the network intrusion detection presented as the sequential expression on the list (table) of the attack signature profile).

As per claim 2 and 3, Vaidya teaches the plurality of signatures includes at least one null signature (Vaidya: Column 11 Line 62 – 65: any signature associated with the expressions with the exception of the last sequential expression is considered as null signature of nominal data without indicating a true network intrusion).

As per claim 4 and 19, Vaidya teaches an intrusion detection method, comprising the steps of:

storing a plurality of signatures in a signature table of an intrusion detection system (Vaidya: Column 3 Line 40 – 45);

detecting, by the intrusion detection system, a system event (Vaidya: Column 3 Line 41 – 48); and

comparing the system event with the plurality of signatures (Vaidya: Column 4 Line 8 – 18);

wherein the step of comparing is performed in a sequence according to a ranking of the plurality of signatures by likelihood of occurrence (Vaidya: Column 11 Line 48 – 51: the likelihood of occurrence is based on the timely sequence of events that may occur during the network intrusion detection presented as the sequential expression on the list (table) of the attack signature profile).

As per claim 5, 9 and 20, Vaidya teaches the ranking of the plurality of signatures by likelihood of occurrence is computed from occurrence data (Vaidya: Column 11 Line 48 – 51, Column 9 Line 3 – 61 and Column 7 Line 52 – 55).

As per claim 6, Vaidya teaches an intrusion detection method, comprising the steps of:

storing a plurality of signatures in a signature table of an intrusion detection system, said plurality of signatures including at least one null signature (Vaidya: Column 3 Line 40 – 45 and Column 11 Line 62 – 65: any signature associated with the expressions with the exception of the last sequential expression is considered as null signature of nominal data without indicating a true network intrusion);

ranking the plurality of signatures by likelihood of occurrence to provide a ranking order (Vaidya: Column 11 Line 48 – 51: the likelihood of occurrence is based on the timely sequence of events that may occur during the network intrusion detection presented as the sequential expression on the list (table) of the attack signature profile);

detecting, by an intrusion detection system, a system event (Vaidya: Column 3 Line 41 – 48); and

comparing the system event with the plurality of signatures (Vaidya: Column 4 Line 8 – 18);

wherein the step of comparing is performed in a sequence according to the ranking order (Vaidya: Column 11 Line 48 – 51).

As per claim 7, Vaidya teaches a method of managing a signature table for an intrusion detection system, comprising the steps of:

detecting, by an intrusion detection system, a system event (Vaidya: Column 3 Line 41 – 48);

determining whether a signature table of the intrusion detection system includes a signature with a signature event that matches the system event (Vaidya: Column 4 Line 8 – 18); and

when the signature table does not include a signature with a signature event that matches the system event, storing, in the signature table, a null signature with a signature event that matches the system event (Vaidya: Column 11 Line 25 – 28: this is the sequential attack signature profile table initiated process as taught by Vaidya).

As per claim 8, Vaidya teaches a method of managing a signature table for an intrusion detection system, comprising the steps of:

detecting, by an intrusion detection system, a system event (Vaidya: Column 3 Line 41 – 48);

determining whether a signature table of the intrusion detection system includes a signature event that matches the system event (Vaidya: Column 4 Line 8 – 18); and

when the signature table includes a signature event that matches the system event, updating occurrence data associated with the signature event (Vaidya: Column 4 Line 22 – 24: a time stamp can also be considered as part of an occurrence data).

As per claim 10, Vaidya teaches when the signature table does not include a signature event that matches the system event, storing a null signature in the signature table (Vaidya: Column 11 Line 25 – 28: this is the sequential attack signature profile table initiated process as taught by Vaidya).

As per claim 11, Vaidya teaches the null signature includes a signature event that matches the system event (Vaidya: Column 11 Line 45 – 65).

5. Claims 12 – 13 are rejected under 35 U.S.C. 102(e) as being anticipated by Hodges (PN: 2002/0112185).

As per claim 12, Hodges teaches an intrusion detection method, comprising the steps of:

detecting, by an intrusion detection system, a system event (Hodges: Para [0246] Line 10 – 22);

determining whether a cache of the intrusion detection system includes a signature event that matches the system event (Hodges: Para [0246] Line 10 – 22);

when the cache does not include the signature event, determining whether a signature table of the intrusion detection system includes the signature event (Hodges: Para [0207] – [0209]); and

when the signature table does not include the signature event, storing the signature event in the cache (Hodges: Para [0209] Line 9 – 11).

As per claim 13, Hodges teaches the signature event is stored in the cache as part of a null signature, and wherein the step of storing includes a step of storing the null signature in the cache (Hodges: Para [0207] Line 8 – 13: the previously stored profile attribute used in a successful authentication is considered as a null signature that does not indicate a threat of intrusive attack).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100